日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　９月２１日

出願番号
Application Number: 特願２００１－２８８０７６

出願人
Applicant(s): 富士通株式会社

２００１年１１月２６日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３１０３１８８

#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of	: **Misao KIMURA**
Filed:	: **Concurrently herewith**
For:	: **COMMUNICATION NETWORK SYSTEM....**
Serial No.	: **Concurrently herewith**

Assistant Commissioner for Patents
Washington, D.C. 20231

January 16, 2002

PRIORITY CLAIM AND SUBMISSION

OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **JAPANESE** patent application no. **2001-288076** filed **September 21, 2001,** a certified copy of which is enclosed.

Any fee, due as a result of this paper, not covered by an enclosed check, may be charged to Deposit Acct. No. 50-1290.

Respectfully submitted,

Samson Helfgott
Reg. No. 23,072

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.: FUJH 19.343
TELEPHONE: (212) 940-8800

【書類名】　特許願
【整理番号】　0151487
【提出日】　平成13年 9月21日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 12/16
H04L 12/22
【発明の名称】　秘匿機能を有する通信ネットワーク・システムおよび通信方法
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　木村　操
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100094514
【弁理士】
【氏名又は名称】　林　恒▲徳▼
【代理人】
【識別番号】　100094525
【弁理士】
【氏名又は名称】　土井　健二
【手数料の表示】
【予納台帳番号】　030708
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9704944

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　秘匿機能を有する通信ネットワーク・システムおよび通信方法

【特許請求の範囲】

【請求項１】　中央管理装置と複数の構内ネットワーク・システムとが相互接続され，前記複数の構内ネットワーク・システムのそれぞれは，ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムであって，

前記中央管理装置は，

少なくとも１つの共通鍵，ならびに，各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと，

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信する中央側暗号部と，

を備え，

前記ルータは，

前記中央側暗号部により送信された，暗号化された前記共通鍵を自己の秘密鍵により復号化する第１のルータ側復号部と，

前記第１のルータ側復号部により復号化された前記共通鍵を記憶する記憶部と，

自己の構内ネットワーク・システムに設けられた第１の送信元端末から他の構内ネットワーク・システムに設けられた第１の送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信するルータ側暗号部と，

を備えている通信ネットワーク・システム。

【請求項２】　中央管理装置と複数の構内ネットワーク・システムとが相互接続され，前記複数の構内ネットワーク・システムのそれぞれは，ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムにおける通信方法であって，

前記中央管理装置は，管理データベースにあらかじめ記憶された少なくとも１つの共通鍵を，管理データベースにあらかじめ記憶された，各ルータにそれぞれ割り当てられた公開鍵により暗号化して，各ルータに送信し，

前記ルータは，

前記中央管理装置から送信された，暗号化された前記共通鍵を自己の秘密鍵により復号化し，

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信する，

通信方法。

【請求項３】　中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ，該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータであって，

前記中央管理装置から送信された，該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵で復号化する復号部と，

前記復号部の復号化により得られた共通鍵を記憶する記憶部と，

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信する暗号部と，

を備えているルータ。

【請求項４】　中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ，該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータの通信方法であって，

前記中央管理装置から送信された，該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵により復号化して自己の記憶部に記憶し，

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネッ

トワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信する，

通信方法。

【請求項５】　ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置であって，

ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間，または，あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも１つの共通鍵，ならびに，各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと，

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信する暗号部と，

を備えている中央管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は，通信データを秘匿する機能を有する通信ネットワーク・システムおよび通信方法に関し，特に，相互接続された複数の構内ネットワーク間で通信されるデータが秘匿される通信ネットワーク・システムおよび通信方法に関する。

【０００２】

また，本発明は，通信データを秘匿する機能を有するルータに関する。さらに，本発明は，通信のデータの秘匿に必要な情報の一元管理を行う中央管理装置に関する。

【０００３】

【従来の技術】

企業等では，１つの建物（ビル，工場等）内にイーサネット・ケーブル等の通信ケーブル（たとえば10BASE-T等）を張り巡らし，このケーブルにその建物内の

端末（クライアント）やサーバ等を接続して構内ネットワーク（ＬＡＮ）ないしはイントラネットを構築することが盛んに行われている。

【０００４】

また，１つの企業等であっても，たとえばその本社，支社，工場等がそれぞれ異なる場所の異なる建物内に存在する場合には，各建物に構築された構内ネットワークをさらに他の通信回線により相互接続して企業内ネットワークを構築している。この各構内ネットワークを相互接続する通信回線として，一般に，通信事業者が提供する専用線（たとえば通信事業者が提供する公衆ネットワークの一部）が用いられる。

【０００５】

このような企業内ネットワークは，インターネットのような開放的で公的なネットワークと異なり，企業等の私的なネットワークであることから，プライベート・ネットワークと呼ばれることがある。

【０００６】

このようなプライベート・ネットワークでは，外部の者に対して秘密の情報，すなわち社外秘の情報（たとえば機密情報，社内情報等）が通信されることがある。このような秘密の情報は，当然のことながら，外部の者による閲覧，複写，改竄等が禁止される。

【０００７】

しかしながら，プライベート・ネットワークの一部を構成する専用線は，建物間を接続するものであるので，建物の外部に敷設される。したがって，このような専用線の部分では，建物内部に敷設された構内ネットワークの部分よりも，外部の者（たとえば不正な第三者）による盗聴，改竄等が行われやすくなっている。

【０００８】

このため，このような盗聴，改竄等から秘密の情報を守るために，種々の暗号化技術が開発され，プライベート・ネットワークにも提供されている。

【０００９】

【発明が解決しようとする課題】

しかし，従来の暗号化の機能は，プライベート・ネットワークの端末（クライアント）に搭載されたメーラやブラウザ等のソフトウェアに組み込まれている。そして，暗号化を行うかどうかは，それを使用するユーザの意識に委ねられている。したがって，各ユーザが情報の秘匿に対して高い意識を持っていなければ，情報の暗号化は行われていないのが実情である。

【００１０】

また，情報の重要度，特に秘匿の対象となる情報であるかどうかは，各ユーザによって異なり，たとえば受信者や第三者にとっては秘匿の対象となる情報であっても，発信者がそのように意識していなければ，暗号化が行われずに送信される。

【００１１】

さらに，プライベート・ネットワークは，建物の外部に敷設された通信回線（たとえば専用線）を使用している部分があるにも関わらず，ユーザは，企業内に閉じたネットワーク（クローズド・ネットワーク）として意識していることが多い。このため，ユーザは，第三者による盗聴，改竄等が行われる危険性を十分に認識していないことが多い。

【００１２】

このような背景から，プライベート・ネットワークにおける情報の暗号化を各個人に委ねるのではなく，システム的にサポートする必要性が高まっている。

【００１３】

また，暗号化を行うときに必要となる暗号鍵／復号鍵を各ユーザが管理するのは煩雑である。たとえば，公開鍵暗号方式では，送信者が送信先（受信者）ごとに異なる公開鍵を管理することが必要となる。また，ネットワークに新たな端末，サーバ，構内ネットワーク等が増設される等のようにシステムが拡張された場合には，これらの増設された端末等の公開鍵を送信者側は新たに管理することが必要となる。このように，送信者側に煩雑な鍵の管理が求められる。

【００１４】

本発明は，このような背景に鑑みなされたものであり，その目的は，複数の構内ネットワーク・システムが相互節則された通信ネットワーク・システムにおい

て，構内ネットワーク間で通信されるデータの秘匿を図ることにある。

【００１５】

また，本発明の目的は，通信データの秘匿に必要な情報の一元的な管理を行うことにある。

【００１６】

【課題を解決するための手段】

前記目的を達成するために，本発明の第１の側面による通信ネットワーク・システムは，中央管理装置と複数の構内ネットワーク・システムとが相互接続され，前記複数の構内ネットワーク・システムのそれぞれは，ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムであって，前記中央管理装置は，少なくとも１つの共通鍵，ならびに，各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと，前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信する中央側暗号部と，を備え，前記ルータは，前記中央側暗号部により送信された，暗号化された前記共通鍵を自己の秘密鍵により復号化する第１のルータ側復号部と，前記第１のルータ側復号部により復号化された前記共通鍵を記憶する記憶部と，自己の構内ネットワーク・システムに設けられた第１の送信元端末から他の構内ネットワーク・システムに設けられた第１の送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信するルータ側暗号部と，を備えている。

【００１７】

本発明の第１の側面による通信方法は，中央管理装置と複数の構内ネットワーク・システムとが相互接続され，前記複数の構内ネットワーク・システムのそれぞれは，ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムにおける通信方法であって，前記中央管理装置は，管理データベースにあらかじめ記憶された少なくとも１つの共通鍵を，管理データベースにあらかじめ記憶された，各ルータにそれぞれ割り当てられた公開鍵により暗号化

して，各ルータに送信し，前記ルータは，前記中央管理装置から送信された，暗号化された前記共通鍵を自己の秘密鍵により復号化し，自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信するものである。

【００１８】

本発明の第１の側面によると，構内ネットワーク・システム間に亘って通信されるデータは，ルータにより暗号化される。したがって，構内ネットワーク・システムの端末のユーザがデータの秘匿（暗号化）を意識しなくても，構内ネットワーク・システム間に亘って通信されるデータを秘匿することができる。これにより，構内ネットワーク・システム間を接続する通信回線におけるデータの秘匿が行われ，該通信回線における第三者による盗聴，複写，改竄等が防止される。

【００１９】

また，暗号化に使用される共通鍵は，中央管理装置の管理データベースに記憶されたものが各ルータに送信され，各ルータにより使用される。したがって，中央管理装置による共通鍵の一元管理が可能となる。

【００２０】

本発明の第２の側面によるルータは，中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ，該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータであって，前記中央管理装置から送信された，該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵で復号化する復号部と，前記復号部の復号化により得られた共通鍵を記憶する記憶部と，自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信する暗号部と，を備えている。

【００２１】

本発明の第２の側面による通信方法は，中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ，該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータの通信方法であって，前記中央管理装置から送信された，該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵により復号化して自己の記憶部に記憶し，自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信するものである。

【００２２】

本発明の第２の側面によっても，前記第１の側面と同様の作用効果を得ることができる。

【００２３】

本発明の第３の側面による中央管理装置は，ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置であって，ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間，または，あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも１つの共通鍵，ならびに，各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと，前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信する暗号部と，を備えている。

【００２４】

本発明の第３の側面によると，構内ネットワーク・システム間で通信されるデータの暗号化に使用される共通鍵を中央管理装置によって一元管理することができる。

【００２５】

【発明の実施の形態】

以下に，本発明の実施の形態について説明するが，これは例であって，本発明の技術的範囲を限定するものではない。

【００２６】

図１は，本発明の実施の形態による通信ネットワーク・システム１０の全体構成を示すブロック図である。この通信ネットワーク・システム１０は，ある企業（企業Ａとする。）のプライベート・ネットワーク・システムであり，専用線ネットワーク１，中央管理装置２，および複数（ｎ個：ｎは２以上の整数）の構内ネットワーク・システム3_1～3_nを備えている。

【００２７】

専用線ネットワーク１は，通信事業者が提供する専用線により構成された通信ネットワークである。この専用線には，公衆ネットワークの一部が割り当てられることもある。

【００２８】

各構内ネットワーク・システム3_1～3_nは，たとえば，企業Ａの本社，工場，営業所等の構内にそれぞれ設置されているイントラネットである。各構内ネットワーク・システム3_1～3_nは，構内ネットワークないしは私設ネットワーク（たとえばイーサネット等のＬＡＮ）4_1～4_n，ルータ5_1～5_n，および，１または２以上の端末6_{11}～6_{1p}…6_{n1}～6_{nq}（ｐおよびｑは１以上の整数）を備えている。

【００２９】

以下では，各構内ネットワーク・システム3_1～3_nを，これらを特に区別して用いる場合を除き，「構内ネットワーク・システム３」と総称する。同様にして，特に区別して用いる場合を除き，私設ネットワーク4_1～4_nを「構内ネットワーク４」と総称し，ルータ5_1～5_nを「ルータ５」と総称し，端末6_{11}～6_{1p}…6_{n1}～6_{nq}を「端末６」と総称する。

【００３０】

各ルータ５および中央管理装置２は，専用線ネットワーク１に接続され，専用線ネットワーク１を介して相互に通信可能に構成されている。また，各構内ネットワーク・システム３に設けられたルータ５および端末６は，構内ネットワーク

４に接続され，相互に通信可能に構成されている。専用線ネットワーク１および構内ネットワーク４を介して通信されるデータ（メッセージ）は，本実施の形態では，ＩＰパケットにより搬送される。端末６は，たとえば企業Ａの経営者，従業員等が使用するパソコン，ワークステーション等であり，クライアントと呼ばれることもある。

【００３１】

ルータ５の代わりに，ファイアウォールが専用線ネットワーク１に接続されることがある。この場合には，ルータ５は，ファイアウォールに接続され，ファイアウォールを介して専用線ネットワーク１に接続されることとなる。

【００３２】

中央管理装置２も，ルータ５と同様に，ある企業の構内に配置されており，構内ネットワーク・システム（構内ネットワーク・システム３_{1}～３_{n}のいずれかまたは異なる構内ネットワーク・システム）に設けられていてもよい。中央管理装置２は，ルータまたはファイアウォールにより構成することができる。

【００３３】

中央管理装置２には，後に詳述する管理データベース２０が設けられている。管理データベース２０は，後に詳述するように，各端末６間で通信されるデータ（ＩＰパケット）の暗号化の必要の有無に関する情報と，暗号化のための鍵に関する情報とを有し，これらの情報を通信ネットワーク・システム１０において一元管理する。管理データベース２０に設けられた情報の一部は，各ルータ５に与えられ，端末６間で通信されるデータの暗号化／復号化の際に使用される。

【００３４】

ある構内ネットワーク・システム３内の端末６（送信元端末）が他の構内ネットワーク・システム３内の端末６(送信先端末)にデータを送信する場合に，このデータは，送信元端末の構内ネットワーク・システム３に設けられたルータ５（送信元ルータ）を経由して専用線ネットワーク１に送信され，専用線ネットワーク１から送信先端末のある構内ネットワーク・システム３のルータ５（送信先ルータ）を経由する。

【００３５】

この際，本実施の形態では，送信元ルータが，送信されるデータを暗号化する必要があるかどうかを判断する。この判断は，管理データベース２０から与えられた情報に基づいて行われる。暗号化の必要がある場合に，送信元ルータはデータを暗号化し，送信先ルータに送信する。

【００３６】

一方，送信先ルータは，送信元ルータから送信されたデータを復号化する必要があるかどうかを判断する。この判断も，管理データベース２０から与えられた情報に基づいて行われる。復号化の必要がある場合に，送信先ルータは，データを復号化し，同じ構内ネットワーク・システムに設けられた送信先端末に，復号化されたデータを送信する。

【００３７】

このように，本実施の形態では，異なる構内ネットワーク・システム３間に亘って通信されるメッセージに対して，ルータ５による暗号化および復号化が行われる。これにより，構内ネットワーク・システム３間に亘って通信されるデータの第三者による盗聴，複写，改竄等が有効に防止される。また，ルータがデータの暗号化／復号化の必要性を判断し，必要な場合には暗号化／復号化を行うので，情報の秘匿を確実に行うことができる。

【００３８】

なお，同一の構内ネットワーク・システム３内で通信されるメッセージに対しては，従来のシステムと同様にして，各端末６のメーラまたはブラウザに設けられた暗号化機能により，暗号化および復号化が行われることとなろう。

【００３９】

以下，管理データベース２０が有する情報の詳細，ルータ５の詳細な構成，および暗号化／復号化の処理の詳細について説明する。

【００４０】

図２～図４は，管理データベース２０が有するデータを示している。管理データベース２０は，秘匿端末テーブル（図２），公開鍵／秘密鍵テーブル（図３（Ａ）または（Ｂ）），および共通鍵テーブル（図４（Ａ）および（Ｂ））のデータを有する。これらのデータは，通信ネットワーク・システム１０の管理者，中

央管理装置２のオペレータ等が中央管理装置２を操作して入力される。

【００４１】

図２を参照して，秘匿端末テーブルは，ルータの欄，加入端末の欄，および相手先端末の欄を有し，端末６間で通信されるデータのうち，秘匿（すなわち暗号化（および復号化））の必要があるデータが送受信される２つの端末（すなわち図２における加入端末および相手先端末）の組み合わせを示している。すなわち，この秘匿端末テーブルに示される加入端末と相手先端末との間でデータが通信される場合に，そのデータは暗号化／復号化されることとなる。

【００４２】

ルータの欄は，通信ネットワーク・システム１０において各ルータ５を識別するための識別情報を有する。この識別情報として，たとえばルータ５のＩＰアドレスが使用される。ただし，この識別情報は通信ネットワーク・システム１０において各ルータ５を識別できる情報であればよいので，ＩＰアドレスの一部や，各ルータ５の名称等がこの識別情報として使用されてもよい。

【００４３】

加入端末の欄は，ルータの欄に設けられたルータ５に加入している（すなわちルータ５に構内ネットワーク４を介して直接接続されている）端末６の識別情報を有する。たとえば端末6_{11}，6_{12}，6_{1p}等は，ルータ5_1に加入しており，該ルータ5_1に構内ネットワーク4_1を介して直接接続されている。

【００４４】

相手先端末の欄は，加入端末の欄に設けられた端末６とデータを通信する際に，秘匿の必要がある通信相手の端末の識別情報を有する。たとえば，加入端末6_{11}と，これに対応する相手先端末6_{21}または6_{25}との間で通信されるデータは秘匿（すなわち暗号化（および復号化））の必要がある。

【００４５】

加入端末が送信元端末となり，相手先端末が送信先端末となる場合もあるし，その逆の場合もある。いずれの場合も，通信されるデータは，秘匿される。

【００４６】

加入端末および相手先端末の欄に格納される識別情報として，たとえば端末６

のＩＰアドレスが使用される。ただし，ルータの欄と同様に，この識別情報は，通信ネットワーク・システム１０において各端末６を識別できる情報であればよいので，ＩＰアドレスの一部，各端末６の名称等が使用されてもよい。

【００４７】

なお，秘匿端末テーブルは，秘匿が必要なデータと秘匿が必要でないデータとを分別するために使用されるので，すべての端末６間で通信されるデータに対して秘匿が必要とされる場合には，この秘匿端末テーブルを管理データベース２０に設ける必要はない。

【００４８】

図３（Ａ）を参照して，公開鍵／秘密鍵テーブルは，中央管理装置２の公開鍵および秘密鍵の組み合わせ，ならびに，各ルータ５の公開鍵および秘密鍵の組み合わせを示すデータである。

【００４９】

ルータの欄には，データおよびこのデータを暗号化するために使用された共通鍵の送信先となるルータ（ルータ５または中央管理装置２）の識別情報が設けられる。公開鍵の欄には，ルータの欄に設けられた送信先ルータに送信されるデータを暗号化および復号化するための共通鍵を暗号化するための公開鍵が設けられる。秘密鍵の欄には，送信先ルータが該共通鍵を復号化するための共通鍵が設けられる。

【００５０】

たとえば，あるルータ５から中央管理装置２へ送信されるデータを暗号化するために使用された共通鍵は，中央管理装置２の公開鍵Ｋpcにより暗号化され，中央管理装置２に送信される。中央管理装置２は，暗号化された共通鍵を秘密鍵Ｋscにより復号化する。同様にして，ルータ５_1以外のルータ５または中央管理装置２からルータ５_1に送信されるデータを暗号化するために使用された共通鍵は，ルータ５_1の公開鍵Ｋp1により暗号化され，ルータ５_1に送信される。ルータ５_1は，暗号化された共通鍵を秘密鍵Ｋs1により復号化する。他のルータの公開鍵および秘密鍵についても同様である。

【００５１】

公開鍵／秘密鍵の組み合わせを，図３（Ｂ）に示すように，相手ルータ（すなわち送信元ルータ（ルータ５または中央管理装置２））ごとに個別に設けることもできる。たとえば，ルータ５_1が中央管理装置２にデータを送信する場合に，ルータ５_1は相手ルータ５_1に対応する公開鍵Ｋpc1により共通鍵を暗号化し，中央管理装置２は相手ルータ$_1$に対応する秘密鍵Ｋsc1により共通鍵を復号化する。他のルータの公開鍵および秘密鍵についても同様である。

【００５２】

図４（Ａ）を参照して，共通鍵テーブルは，複数の共通鍵から構成される。各ルータ５および中央管理装置２は，この複数の共通鍵の中から任意の１つを選択して，メッセージを暗号化する。選択の方法は，各ルータ５および中央管理装置２に委ねられる。

【００５３】

図４（Ｂ）に示すように，共通鍵テーブルには，共通鍵の欄に加えて，各共通鍵に対応した共通鍵暗号方法（共通鍵暗号方式）を設けることができる。たとえば，共通鍵Ｋc1には暗号方法Ｍ１が，共通鍵Ｋc2には暗号方法Ｍ２が，それぞれ使用される。各共通鍵に対応する暗号化方法は，他の共通鍵に対応する暗号方法と同じものであってもよいし，異なるものであってもよい。共通鍵暗号方法には，ＤＥＳ（Data Encryption Standard），ＡＥＳ（Advanced Encryption Standard）等がある。

【００５４】

管理データベース２０に格納されたこれらのデータ（テーブル）の一部は，中央管理装置２から専用線ネットワーク１を介して各ルータ５に送信され，各ルータ５の内部メモリ（半導体メモリ，ハードディスク等）に記憶される。この送信は，送信するデータを，管理データベース２０に記憶された共通鍵（図４（Ａ）または（Ｂ）参照）の１つにより暗号化するとともに，該共通鍵を，送信先となるルータ５の公開鍵により暗号化して，送信するデータに付加して行われる。受信側のルータ５は，暗号化された共通鍵を自己の秘密鍵により復号化し，この復号化された共通鍵により，暗号化されたデータを復号化する。これらの送受信の処理は，後述する図８および図９のフローチャートに示すものと同様である。

【００５５】

図５は，ルータ５のうちルータ５_1を例にとり，該ルータ５_1が有するデータを示している。同図（Ａ）は秘匿端末テーブルを，同図（Ｂ）は公開鍵／秘密鍵テーブルを，同図（Ｃ）は共通鍵テーブルを，それぞれ示している。

【００５６】

図５（Ａ）を参照して，参照ルータ５_1が有する秘匿端末テーブルは，管理データベース２０が有する秘匿端末テーブル（図２参照）のうち，ルータの欄がルータ５_1に関する部分のみを有する。すなわち，ルータ５_1が有する秘匿端末テーブルは，ルータ５_1の加入端末とその相手先端末との対応表の部分のみを有する。

【００５７】

図５（Ｂ）を参照して，ルータ５_1が有する公開鍵／秘密鍵テーブルは，管理データベース２０が有する公開鍵／秘密鍵テーブル（図３（Ａ）参照）のうち，自身（すなわちルータ５_1）の公開鍵および秘密鍵，ならびに他のルータ５および中央管理装置２の公開鍵のみを有する。公開鍵／秘密鍵テーブルが図３（Ｂ）に示すものである場合には，ルータ５_1が有する公開鍵／秘密鍵テーブルも，同様に，相手ルータごとに個別に設けられる。

【００５８】

図５（Ｃ）を参照して，ルータ５_1が有する共通鍵テーブルは，管理データベース２０が有するもの（図４（Ａ）または（Ｂ）参照）と同じである。

【００５９】

他のルータ５_2～５_nが有するテーブルも，ルータ５_1が有するテーブルと同様である。

【００６０】

これらのテーブル以外に，各ルータ５は，ルータであるので，経路制御を行うためのルーティング・テーブル等，一般のルータが備えているデータを有することはいうまでもない。

【００６１】

各ルータ５は，このようなテーブルに基づいて，通信データの暗号化および復

号化を行い，暗号化されたデータのルーティングおよび加入端末への配信を行う。図６は，加入端末６（送信元端末）からデータを受信した送信元ルータが送信先ルータの加入端末６（送信先端末）に該データを送信する場合の処理の流れを示すフローチャートである。

【００６２】

送信元ルータが，構内ネットワーク４を介して自身に直接接続された送信元端末からデータ（ＩＰパケット）を受信すると（ステップＳ１でＹＥＳ），該送信元ルータは，該メッセージが秘匿（すなわち暗号化）の対象かどうかを判断する（ステップＳ２）。

【００６３】

この判断は，データのヘッダ部に含まれる送信元端末のＩＰアドレスおよび送信先端末のＩＰアドレスと，自身に記憶されている秘匿端末テーブル（図５（Ａ）参照）とを比較することにより行われる。送信元端末のＩＰアドレスおよび送信先端末のＩＰアドレスの組み合わせが秘匿端末テーブルに存在する場合には，そのデータは秘匿対象であると判断され，存在しない場合には，そのデータは秘匿対称でないと判断される。

【００６４】

データが秘匿対象であると判断されると（ステップＳ２でＹＥＳ），送信元ルータは，ルーティング・テーブルに基づいて，送信先ルータを特定し，特定した送信先ルータの公開鍵を，自身に記憶されている公開鍵／秘密鍵テーブル（図５（Ｂ）参照）から選択する（ステップＳ３）。

【００６５】

続いて，送信元ルータは，データを暗号化するための共通鍵を，自身に記憶された共通鍵テーブル（図５（Ｃ）参照）から選択する（ステップＳ４）。そして，送信側ルータは，選択した共通鍵を用いてデータ（本実施の形態では，ＩＰパケットのデータ部のみ）を暗号化する（ステップＳ５）。

【００６６】

次に，送信元ルータは，ステップＳ３で選択された公開鍵を用いて，データ部の暗号に使用された共通鍵を暗号化し（ステップＳ６），この暗号化された共通

鍵をＩＰパケットのデータ部に付加する。暗号化された共通鍵をデータ部のどの箇所に付加するかは，送信元ルータと送信先ルータとの間であらかじめ定められている。たとえば，データ部の先頭，最後尾等の箇所に，暗号化された共通鍵が付加される。

【００６７】

次に，送信元ルータは，暗号化された共通鍵をデータ部に付加することに伴って生じる，ＩＰパケットのヘッダ部の変更を行う（ステップＳ８）。変更を行う箇所として，ＩＰｖ４の場合には，ヘッダ部のヘッダ長，全長，ＩＤ，およびフラグがある。これらの各値が，暗号化された共通鍵を付加した後の値に変更される。

【００６８】

続いて，送信元ルータは，このＩＰパケットを専用線ネットワーク１を介して送信先ルータに送信する（ステップＳ９）。その後，処理は，ステップＳ１に戻る。なお，ＩＰパケットが送信元ルータから送信先ルータに届くまでに１または2以上の中継ルータ（ルータ５のいずれか）を経由する場合には，これらの中継ルータは，インターネットにおける一般の中継ルータと同様に，ルーティング・テーブルに基づいて，ＩＰパケットをルーティングする。

【００６９】

ステップＳ２において，データが秘匿対称でないと判断されると（ステップＳ２でＮＯ），処理はステップＳ９に進み，データは暗号化等の処理を受けることなく，そのまま送信元ルータから送信される。

【００７０】

なお，すべてのデータが暗号化の対象となる場合には，ステップＳ２の処理は省略される。

【００７１】

図７は，送信先ルータの処理の流れを示すフローチャートである。送信先ルータは，送信元ルータからデータ（ＩＰパケット）を受信すると（ステップＳ１１），受信したデータが秘匿対象であるかどうかを判断する（ステップＳ１２）。この判断は，前述したステップＳ２の判断と同様に，ＩＰパケットのヘッダ部に

含まれる発信元アドレス（ＩＰアドレス）および宛先アドレス（ＩＰアドレス）と，自己に記憶された秘匿対象テーブル（図５（Ａ）参照）とを比較することにより行われる。

【００７２】

データが秘匿対象であると判断された場合には（ステップＳ１２でＹＥＳ），送信先ルータは，自己に記憶された公開鍵／秘密鍵テーブル（図５（Ｂ）参照）から，自己の秘密鍵を選択する（ステップＳ１３）。

【００７３】

次に，送信先ルータは，暗号化された共通鍵を，データ（ＩＰパケット）のデータ部から抽出する（ステップＳ１４）。前述したように，暗号化された共通鍵が付加された箇所はルータ間であらかじめ定められているので，送信先ルータは，このあらかじめ定められた箇所から共通鍵を抽出する。

【００７４】

続いて，送信先ルータは，抽出された共通鍵を，ステップＳ１３で選択された秘密鍵により復号化する（ステップＳ１５）．そして，送信先ルータは，復号化により得られた共通鍵により，データ部を復号化する（ステップＳ１６）。図４（Ｂ）に示すように，共通鍵に対応して暗号化方法が定められている場合には，送信先ルータは，自己に記憶された共通鍵テーブルから，復号化された共通鍵に対応する暗号化方法を選択し，この共通鍵および選択された暗号化方法に基づいて，データ部を復号化する。

【００７５】

続いて，送信先ルータは，データ部の復号化およびデータ部からの共通鍵の抽出に伴い生じるＩＰパケットのヘッダ部の変更（すなわち暗号化前の状態に復元）を行う（ステップＳ１７）。

【００７６】

その後，送信先ルータは，復元されたＩＰパケットを，自己に直接接続された送信先端末（加入端末）に構内ネットワーク４を介して送信する（ステップＳ１８）。その後，処理は，ステップＳ１１に戻る。

【００７７】

ステップＳ１２において，データが秘匿対称でないと判断されると（ステップＳ２でＮＯ），処理はステップＳ１８に進み，データは復号化等の処理を受けることなく，そのまま端末に送信される。

【００７８】

なお，すべてのデータが復号化の対象となる場合には，ステップＳ１２の処理は省略される。

【００７９】

このように，本実施の形態では，ルータ５が，あらかじめ定められた秘匿端末テーブルに基づいてデータを暗号化／復号化するので，端末６のユーザが特に秘匿を意識しなくても，情報（たとえば社外秘の情報等）を第三者の盗聴，複写，改竄等から有効に守ることができる。

【００８０】

次に，管理データベース２０に記憶されたテーブルが更新された場合の各ルータに記憶されたテーブルの更新処理について説明する。

【００８１】

通信ネットワーク・システム１０の暗号化／復号化に必要な情報は，中央管理装置２および管理データベース２０によって一元管理されるので，この情報に変更が生じると，まず管理データベース２０の情報が更新される。

【００８２】

この管理データベース２０の更新は，ある構内ネットワーク・システム３に新たな端末６が追加された場合，ある構内ネットワーク・システム３から既設の端末６が取り除かれた場合，新たな構内ネットワーク・システム３が通信ネットワーク・システム１０に追加された場合，既設の構内ネットワーク・システム３が通信ネットワーク・システム１０から取り除かれた場合，公開鍵，秘密鍵，または共通鍵に追加，変更，または削除が生じた場合等に行われる。

【００８３】

たとえば，ある構内ネットワーク・システム３に新たな端末６が追加された場合に，新たに追加された端末に関する情報が秘匿対象テーブル（図２参照）に追加される。また，新たな構内ネットワーク・システム３が追加された場合には，

秘匿対象テーブルには，新たに追加された構内ネットワーク・システム３のルータ５および端末６に関する情報が追加され，公開鍵／秘密鍵テーブル（図３（Ａ）または（Ｂ）参照）には，新たに追加された構内ネットワーク・システム３のルータ５に関する情報（公開鍵および秘密鍵）が追加される。公開鍵または秘密鍵に変更が生じた場合には，公開鍵／秘密鍵テーブルが変更され，共通鍵（または暗号化方法）に変更が生じた場合には，共通鍵テーブル（図４（Ａ）または（Ｂ）参照）が変更される。

【００８４】

また，これらの場合に加えて，管理データベース２０は，同一の状態が長期間継続することを避け，セキュリティを高めるために，定期的に更新されることが好ましい。

【００８５】

この管理データベース２０の更新は，通信ネットワーク・システム１０の管理者，中央管理装置２のオペレータ等が中央管理装置２を操作することにより行われる。

【００８６】

管理データベース２０が更新されると，管理データベース２０の更新を各ルータ５に記憶されたテーブルにも反映させるために，更新された部分が更新の必要なルータ５に送信される。図８は，管理データベース２０の秘匿対象テーブル，公開鍵／秘密鍵テーブル，または共通鍵テーブルが更新された場合における中央管理装置２の処理の流れを示すフローチャートである。

【００８７】

まず，中央管理装置２は，更新されたテーブルを送信する対象となるルータ（送信先ルータ）のテーブルを作成する（ステップＳ２１）。

【００８８】

続いて，中央管理装置２は，送信先ルータの公開鍵を公開鍵／秘密鍵テーブルから選択する（ステップＳ２２）。ここで，公開鍵／秘密鍵テーブルが更新されている場合には，公開鍵が選択される公開鍵／秘密鍵テーブルは更新前のものである（すなわち，選択される公開鍵も更新前のものである）ことが好ましい。こ

れは，更新された公開鍵／秘密鍵テーブルを受信する送信先ルータは，更新された公開鍵／秘密鍵を受信し，自己のデータの更新が完了するまでは，更新前の秘密鍵を用いて復号化を行うからである。したがって，管理データベース２０には，各ルータに記憶されたデータの更新が完了するまでは，更新前のデータも一時的に保持されることが好ましい。

【００８９】

続いて，中央管理装置２は，送信先ルータの共通鍵を共通鍵テーブルから選択する（ステップＳ２３）。ここで，前述した公開鍵／秘密鍵テーブルと同様に，共通鍵テーブルについても，更新されている場合には，共通鍵が選択される共通鍵テーブルは更新前のものである（すなわち，選択される共通鍵も更新前のものである）ことが好ましい。

【００９０】

次に，中央管理装置２は，ステップＳ２３で選択された共通鍵により，ステップＳ２１において準備されたテーブルから作成されたＩＰパケットのデータ部を暗号化する（ステップＳ２４）。準備されたテーブルが複数のＩＰパケットに分割される場合には，各ＩＰパケットのデータ部が共通鍵により暗号化される。

【００９１】

続いて，中央管理装置２は，ステップＳ２２で選択された公開鍵により，共通鍵を暗号化する（ステップＳ２５）。

【００９２】

続いて，前述した図６のステップＳ７の処理と同様に，中央管理装置２は，暗号化された共通鍵をＩＰパケットのデータ部に付加する（ステップＳ２６）。これに伴い，付加されたＩＰパケットのヘッダ部が変更される。テーブルが複数のＩＰパケットに分割されて送信される場合に，暗号化された共通鍵は，先頭のＩＰパケットに付加されることが好ましい。

【００９３】

続いて，中央管理装置２は，これらの暗号化されたテーブルおよび共通鍵を送信先ルータに送信する（ステップＳ２７）。

【００９４】

一方，送信先ルータは，更新されたテーブルが送信されると，このテーブルにより，自己に記憶されたデータを更新する。図９は，更新されたテーブルが中央管理装置２から送信された場合における送信先ルータの処理の流れを示すフローチャートである。

【００９５】

送信先ルータは，暗号化されたテーブルおよび共通鍵を中央管理装置２から受信すると（ステップＳ３１），秘密鍵を選択し（ステップＳ３２），暗号化された共通鍵を選択した秘密鍵により復号化する（ステップＳ３３）。ここで，中央管理装置２から送信されたテーブルが公開鍵／秘密鍵テーブルであり，公開鍵／秘密鍵テーブルを更新する場合であっても，ステップＳ３２で選択される秘密鍵は，送信先ルータに既に記憶されているもの（すなわち更新前のもの）である。

【００９６】

続いて，送信先ルータは，共通鍵でテーブルを復号化する（ステップＳ３４）。テーブルが複数のＩＰパケットに分割され，送信されている場合には，各ＩＰパケットのデータ部が復号化され，復号化された複数のデータ部を結合することにより，テーブルが再構築されることとなる。

【００９７】

続いて，送信先ルータは，復号化されたテーブルにより，自己に記憶されたテーブルを置換（更新）する（ステップＳ３５）。これにより，送信先ルータのテーブルの更新が終了する。

【００９８】

このように，本実施の形態では，秘匿端末テーブル，公開鍵／秘密鍵テーブル，および共通鍵テーブルが中央管理装置２および管理データベース２０によって一元管理される。そして，更新された場合には，更新された情報が，中央管理装置２から各ルータ５に送信され，ルータ５の保持するデータが更新される。したがって，端末６のユーザが鍵を管理したり，データの暗号化／復号化の必要の有無を判断したりする煩雑さが解消される。また，通信ネットワーク・システム１０に変更が生じたい場合にも，この変更に柔軟に対応することができる。

【００９９】

これまで述べた実施の形態では，ＩＰパケット単位で暗号化を行っているが，送信対象となるデータ全体を先に暗号化し，暗号化されたデータ全体をＩＰパケットに分割して送信することもできる。また，送信元ルータによって使用される共通鍵が送信先ルータにあらかじめ判明している場合には，この共通鍵は，公開鍵により暗号化されて送信先ルータに送信されなくてもよい。

【０１００】

なお，図６から図９に示す各フローチャートの処理は，ルータ５または中央管理装置２に組み込まれるプログラムにより記述することもできるし，ハードウェア回路により実現することもできる。

【０１０１】

（付記１）　中央管理装置と複数の構内ネットワーク・システムとが相互接続され，前記複数の構内ネットワーク・システムのそれぞれは，ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムであって，

前記中央管理装置は，

少なくとも１つの共通鍵，ならびに，各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと，

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信する中央側暗号部と，

を備え，

前記ルータは，

前記中央側暗号部により送信された，暗号化された前記共通鍵を自己の秘密鍵により復号化する第１のルータ側復号部と，

前記第１のルータ側復号部により復号化された前記共通鍵を記憶する記憶部と，

自己の構内ネットワーク・システムに設けられた第１の送信元端末から他の構内ネットワーク・システムに設けられた第１の送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記

中央管理装置に向けて送信するルータ側暗号部と，

を備えている通信ネットワーク・システム。

【０１０２】

（付記２）　付記１において，

前記中央側暗号部は，前記公開鍵をさらに暗号化して各ルータに送信し，

前記第１のルータ側復号部は，前記中央側暗号部により暗号化された前記公開鍵を自己の秘密鍵により復号化し，

前記記憶部は，前記復号化された公開鍵を記憶し，

前記ルータ側暗号部は，前記記憶部に記憶された公開鍵から，前記送信先となる他の構内ネットワーク・システムのルータまたは前記中央管理装置の公開鍵を選択し，該選択した公開鍵により前記共通鍵を暗号化し，該暗号化された共通鍵を前記暗号化された通信データとともに前記他の構内ネットワークまたは前記中央管理装置に向けて送信する，

通信ネットワーク・システム。

【０１０３】

（付記３）　付記１または２において，

前記管理データベースは，前記複数の構内ネットワーク・システムのあるものの端末と他のものの端末との組み合わせのうち，これらの端末間の通信データを暗号化する必要がある組み合わせを示す秘匿端末データをさらに記憶し，

前記中央側暗号部は，前記秘匿端末データを各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信し，

前記第１のルータ側復号部は，前記中央側暗号部により送信された，暗号化された前記秘匿端末データを自己の秘密鍵により復号化し，

前記記憶部は，前記復号化された秘匿端末データを記憶し，

前記ルータ側暗号部は，前記第１の送信元端末および前記第１の送信先端末の組み合わせが前記秘匿端末データに含まれている場合には，前記通信データを暗号化し，含まれていない場合には前記通信データを暗号化しない，

通信ネットワーク・システム。

【０１０４】

（付記４）　付記１または２において，

前記ルータは，他の構内ネットワーク・システムに設けられた第２の送信元端末から自己の構内ネットワーク・システムに設けられた第２の送信先端末に送信されてきたデータを復号化して，該自己の構内ネットワーク・システムに設けられた前記第２の送信先端末に送信する第２のルータ側復号部をさらに備えている通信ネットワーク・システム。

【０１０５】

なお，ここで，第２の送信元端末と第１の送信先端末とは，同じ端末であってもよいし，異なる端末であってもよい。同様にして，第２の送信先端末と第１の送信元端末とは，同じ端末であってもよいし，異なる端末であってもよい。

【０１０６】

（付記５）　付記４において，

前記管理データベースは，前記複数の構内ネットワーク・システムのあるものの端末と他のものの端末との組み合わせのうち，これらの端末間の通信データを暗号化する必要がある組み合わせを示す秘匿端末データをさらに記憶し，

前記中央側暗号部は，前記秘匿端末データを各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信し，

前記第１のルータ側復号部は，前記中央側暗号部により送信された，暗号化された前記秘匿端末データを自己の秘密鍵により復号化し，

前記記憶部は，前記復号化された秘匿端末データを記憶し，

前記第２のルータ側復号部は，前記第２の送信元端末および前記第２の送信先端末の組み合わせが前記秘匿端末データに含まれている場合には，前記通信データを復号化し，含まれていない場合には前記通信データを復号化しない，

通信ネットワーク・システム。

【０１０７】

（付記６）　付記１において，

前記管理データベースに記憶された共通鍵が更新された場合に，前記中央側暗号部は更新された共通鍵を暗号化して送信し，前記第１のルータ側復号部は更新された共通鍵を復号化し，前記記憶部はすでに記憶された共通鍵を更新された共

通鍵に置換して記憶する，通信ネットワーク・システム。

【０１０８】

（付記７）　付記２において，

前記管理データベースに記憶された公開鍵が更新された場合に，前記中央側暗号部は更新された公開鍵を暗号化して送信し，前記第１のルータ側復号部は更新された公開鍵を復号化し，前記記憶部はすでに記憶された公開鍵を更新された公開鍵に置換して記憶する，通信ネットワーク・システム。

【０１０９】

（付記８）　付記３または５において，

前記管理データベースに記憶された前記秘匿端末データが更新された場合に，前記中央側暗号部は更新された秘匿端末データを暗号化して送信し，前記第１のルータ側復号部は更新された秘匿端末データを復号化し，前記記憶部はすでに記憶された秘匿端末データを更新された秘匿端末データに置換して記憶する，通信ネットワーク・システム。

【０１１０】

（付記９）　中央管理装置と複数の構内ネットワーク・システムとが相互接続され，前記複数の構内ネットワーク・システムのそれぞれは，ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムにおける通信方法において，

前記中央管理装置は，管理データベースにあらかじめ記憶された少なくとも１つの共通鍵を，管理データベースにあらかじめ記憶された，各ルータにそれぞれ割り当てられた公開鍵により暗号化して，各ルータに送信し，

前記ルータは，

前記中央管理装置から送信された，暗号化された前記共通鍵を自己の秘密鍵により復号化し，

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信する，

通信方法。

【０１１１】

（付記１０）　中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ，該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータであって，

前記中央管理装置から送信された，該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵で復号化する復号部と，

前記復号部の復号化により得られた共通鍵を記憶する記憶部と，

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信する暗号部と，

を備えているルータ。

【０１１２】

（付記１１）　中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ，該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータの通信方法であって，

前記中央管理装置から送信された，該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵により復号化して自己の記憶部に記憶し，

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信する，

通信方法。

【０１１３】

（付記１２）　中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ，該構内ネットワーク・システムのそれぞれに設けら

れた端末と構内ネットワークを介して接続されたルータに，

前記中央管理装置から送信された，該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵により復号化して自己の記憶部に記憶する手順と，

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ，または，自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して，前記他の構内ネットワークまたは前記中央管理装置に向けて送信する手順と，

を実行させるためのプログラム。

【０１１４】

（付記１３）　ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置であって，

ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間，または，あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも１つの共通鍵，ならびに，各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと，

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信する暗号部と，

を備えている中央管理装置。

【０１１５】

（付記１４）　ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置の管理方法であって，

ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間，または，あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも１つの共通鍵，ならびに，各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を管理データベースに記憶して管理し，

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信する，

管理方法。

【０１１６】

（付記１５）　ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置に設けられたコンピュータに，

ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間，または，あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも１つの共通鍵，ならびに，各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を管理データベースに記憶して管理させる手順と，

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して，各ルータに送信する手順と，

を実行させるためのプログラム。

【０１１７】

【発明の効果】

本発明によると，構内ネットワーク・システム間で通信されるデータの秘匿を各端末のユーザが特に意識しなくても，暗号化の必要なデータは暗号化されて送信され，受信側において復号化されて配信される。これにより，構内ネットワーク・システム間で通信されるデータを秘匿することができる。

【０１１８】

また，本発明によると，構内ネットワーク・システム間で通信されるデータの秘匿に必要な情報（共通鍵，公開鍵，秘密鍵等）を中央管理装置によって一元管理することができる。これにより，各ユーザ，ルータ等で個別に秘匿情報を管理することが不要となり，また，通信ネットワーク・システムの変更に対して柔軟に対処することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態による暗号通信ネットワーク・システムの全体構成を示すブロック図である。

【図２】

管理データベースが有するデータ（秘匿端末テーブル）を示す。

【図３】

管理データベースが有するデータ（公開鍵／共通鍵テーブル）を示す。

【図４】

管理データベースが有するデータ（共通鍵テーブル）を示す。

【図５】

各ルータが有するデータを示し，（Ａ）は秘匿端末テーブルを，（Ｂ）は公開鍵／秘密鍵テーブルを，（Ｃ）は共通鍵テーブルを，それぞれ示す。

【図６】

送信元ルータの処理の流れを示すフローチャートである。

【図７】

送信先ルータの処理の流れを示すフローチャートである。

【図８】

管理データベースの秘匿対象テーブル，公開鍵／秘密鍵テーブル，または共通鍵テーブルが更新された場合における中央管理装置の処理の流れを示すフローチャートである。

【図９】

更新されたテーブルが中央管理装置から送信された場合における送信先ルータの処理の流れを示すフローチャートである。

【符号の説明】

１０　通信ネットワーク・システム（プライベート・ネットワーク・システム）

１　専用線ネットワーク

２　中央管理装置

3_1～3_n　構内ネットワーク・システム

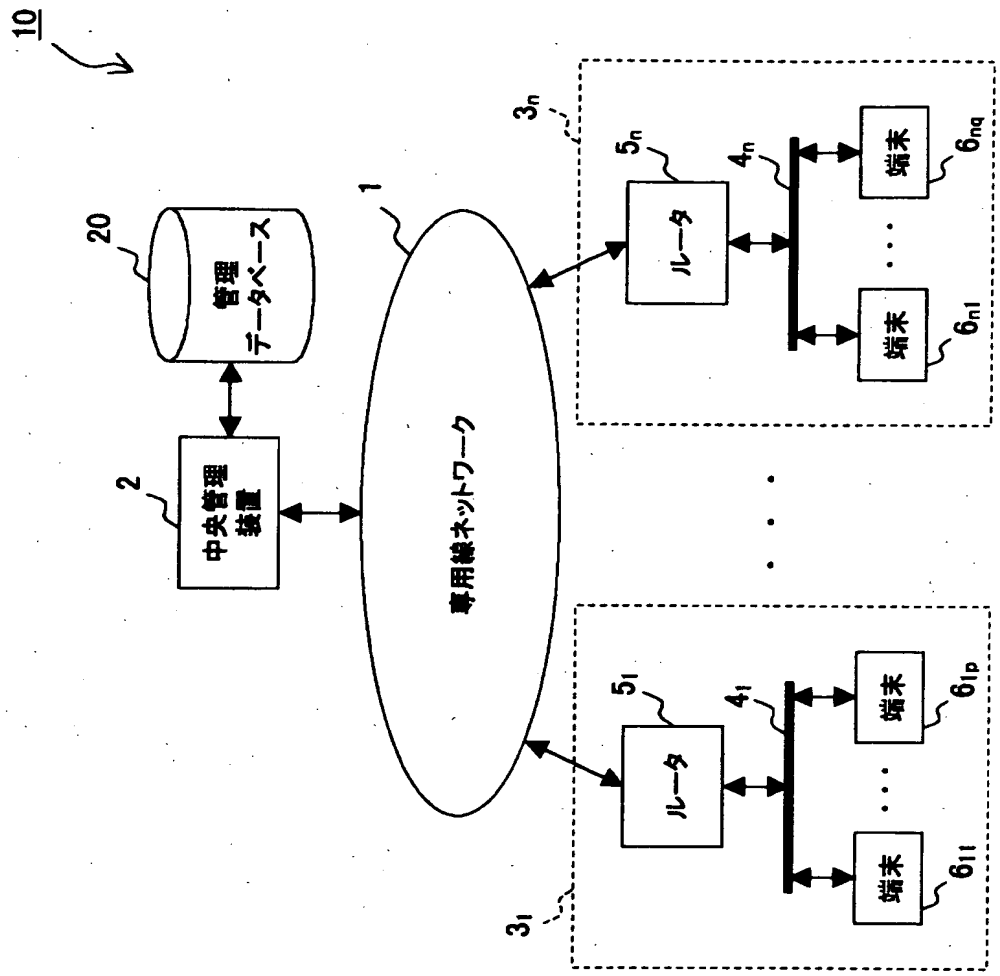
4_1～4_n　構内ネットワーク

5_1～5_n　ルータ

6_{11}～6_{1p}，6_{n1}～6_{nq}　端末

【書類名】　　図面

【図１】


10
20
管理データベース
2
中央管理装置
1
専用線ネットワーク
3n
5n
ルータ
4n
端末
6nq
端末
6n1
3l
5l
ルータ
4l
端末
6lp
端末
6l1

【図２】

秘匿端末テーブル

ルータ	加入端末	相手先端末
ルータ5_1	端末6_{11}	端末6_{21}
	端末6_{11}	端末6_{25}
	・ ・ ・	・ ・ ・
	端末6_{12}	端末6_{32}
	端末6_{12}	端末6_{44}
	・ ・ ・	・ ・ ・
	端末6_{1p}	端末6_{22}
	・ ・ ・	・ ・ ・
ルータ5_2	・ ・ ・	・ ・ ・
・ ・ ・	・ ・ ・	・ ・ ・
ルータ5_n	・ ・ ・	・ ・ ・

【図３】

(A)公開鍵／秘密鍵テーブル

ルータ	公開鍵	秘密鍵
中央管理装置	Kpc	Ksc
ルータ5_1	Kp1	Ks1
ルータ5_2	Kp2	Ks2
・ ・ ・	・ ・ ・	・ ・ ・
ルータ5_n	Kpn	Ksn

(B)公開鍵／秘密鍵テーブル

ルータ	相手ルータ	公開鍵	秘密鍵
中央管理装置	ルータ5_1	Kpc1	Ksc1
	ルータ5_2	Kpc2	Ksc2
	・ ・ ・	・ ・ ・	・ ・ ・
	ルータ5_n	Kpcn	Kscn
ルータ5_1	中央管理装置	Kp1c	Ks1c
	ルータ5_2	Kp12	Ks12
	・ ・ ・	・ ・ ・	・ ・ ・
	ルータ5_n	Kp1n	Ks1n
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

【図４】

(A)共通鍵テーブル

共通鍵
Kc1
Kc2
・ ・ ・

(B)共通鍵テーブル

共通鍵	暗号方法
Kc1	M1
Kc2	M2
・ ・ ・	・ ・ ・

【図５】

(A)秘匿端末テーブル

加入端末	相手先端末
端末6_{11}	端末6_{21}
端末6_{11}	端末6_{25}
・ ・ ・	・ ・ ・
端末6_{12}	端末6_{32}
端末6_{12}	端末6_{44}
・ ・ ・	・ ・ ・
端末6_{1p}	端末6_{22}
・ ・ ・	・ ・ ・

(B)公開鍵／秘密鍵テーブル

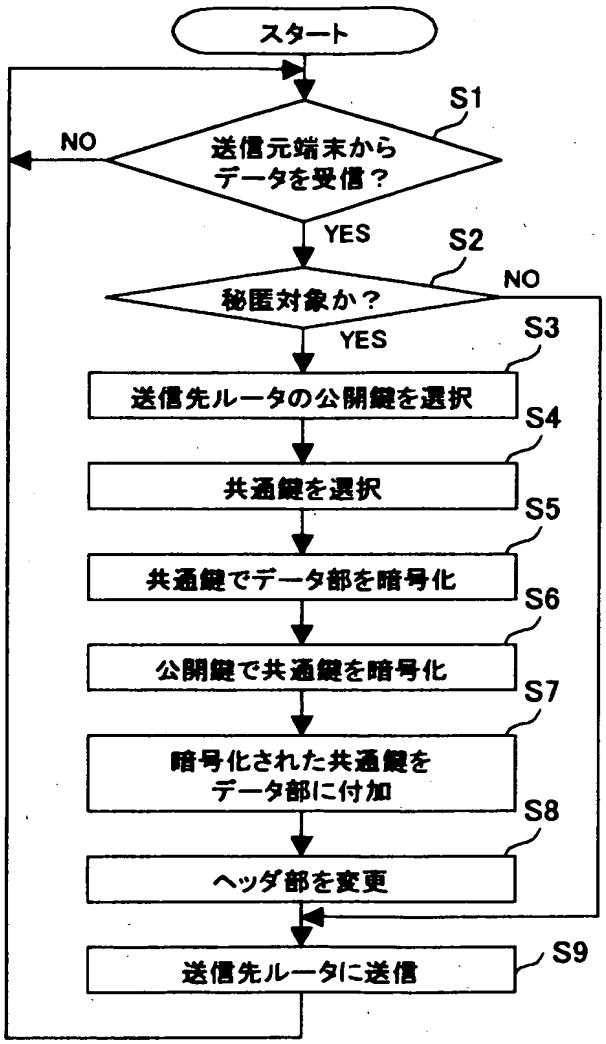
ルータ	公開鍵	秘密鍵
ルータ5_1	Kp1	Ks1
ルータ5_2	Kp2	
・ ・ ・	・ ・ ・	・ ・ ・
ルータ5_n	Kpn	
中央管理装置	Kpc	

(C)共通鍵テーブル

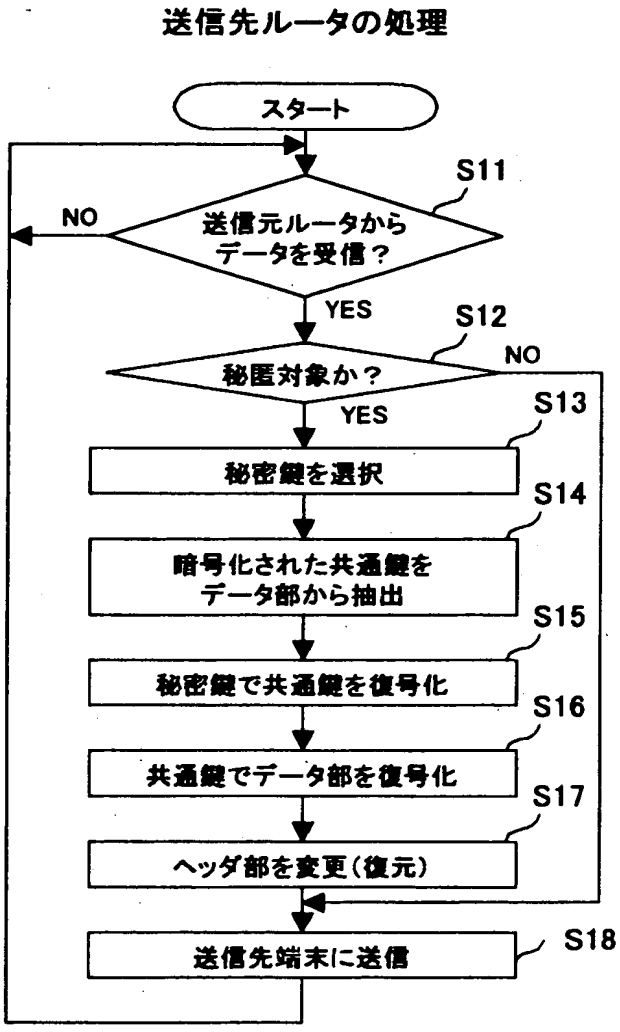
共通鍵
Kc1
Kc2
・ ・ ・

【図６】

送信元ルータの処理

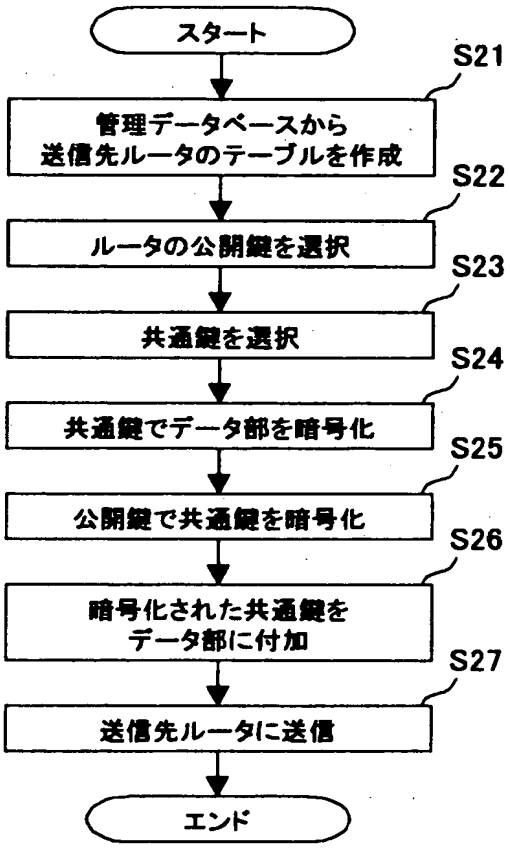


【図７】


送信先ルータの処理
スタート
S11
送信元ルータから
データを受信？
NO
YES
S12
秘匿対象か？
NO
YES
S13
秘密鍵を選択
S14
暗号化された共通鍵を
データ部から抽出
S15
秘密鍵で共通鍵を復号化
S16
共通鍵でデータ部を復号化
S17
ヘッダ部を変更（復元）
S18
送信先端末に送信

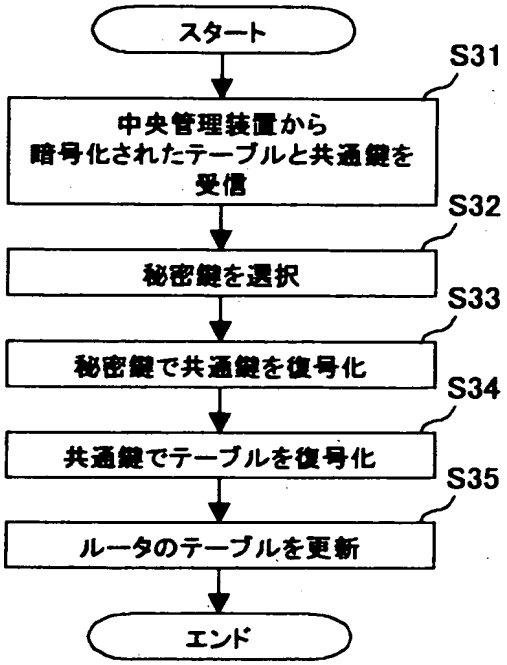
【図８】

テーブルの更新処理（中央管理装置）



【図９】

テーブルの更新処理（ルータ側）



【書類名】　　要約書

【要約】

【課題】　複数の構内ネットワーク・システムが相互節則された通信ネットワーク・システムにおいて，構内ネットワーク間で通信されるデータの秘匿を図る。

【解決手段】　通信ネットワーク・システム１０では，中央管理装置２と複数の構内ネットワーク・システム３とが相互接続され，各構内ネットワーク・システム３では，ルータ５と端末６とが接続されている。中央管理データベース２０は，共通鍵と，各ルータ５および該中央管理装置２にそれぞれ割り当てられた公開鍵とを記憶する。中央管理装置２は，共通鍵を各ルータ５の公開鍵により暗号化して送信する。ルータ５は，暗号化された共通鍵を自己の秘密鍵により復号化し，復号化された共通鍵を記憶する。各ルータ５は，自己の構内ネットワーク・システム３に設けられた送信元端末６から他の構内ネットワーク・システム３に設けられた送信先端末６へ送信される通信データ共通鍵により暗号化して送信する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００１－２８８０７６
受付番号	５０１０１３９２８１７
書類名	特許願
担当官	金井　邦仁　　３０７２
作成日	平成１３年１０月　２日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】	富士通株式会社

【代理人】　申請人

【識別番号】	100094514
【住所又は居所】	神奈川県横浜市港北区新横浜３－９－５　第三東昇ビル３階　林・土井　国際特許事務所
【氏名又は名称】	林　恒徳

【代理人】

【識別番号】	100094525
【住所又は居所】	神奈川県横浜市港北区新横浜３－９－５　第三東昇ビル３階　林・土井　国際特許事務所
【氏名又は名称】	土井　健二

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社